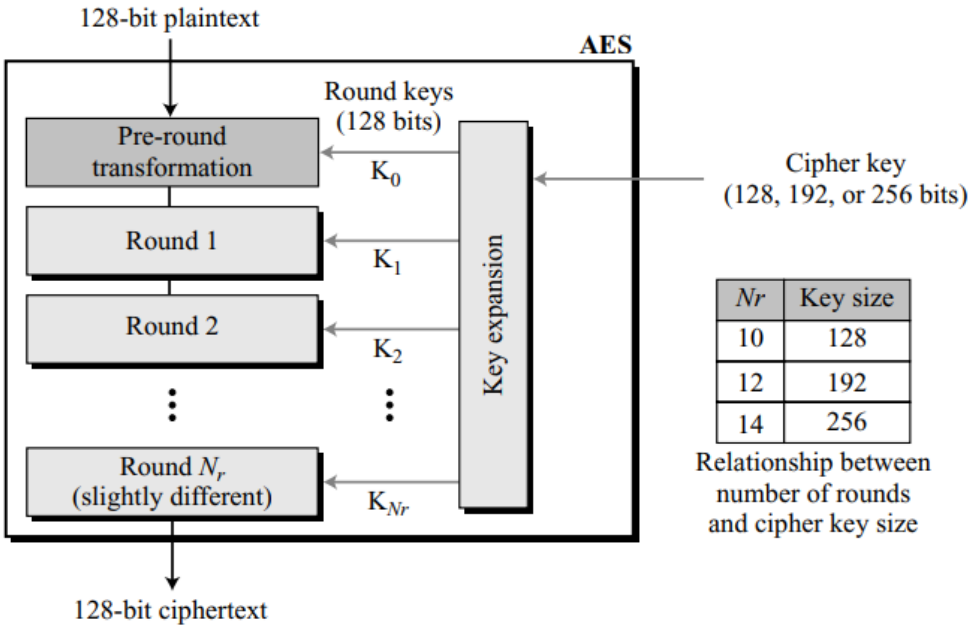
AC Chapter 3 II

Created	@November 23, 2023 4:14 PM
Reviewed	☐

AES (Advanced Encryption Standards)

AES was published by NIST in December 2001. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds.

Figure 7.1 *General design of AES encryption cipher*

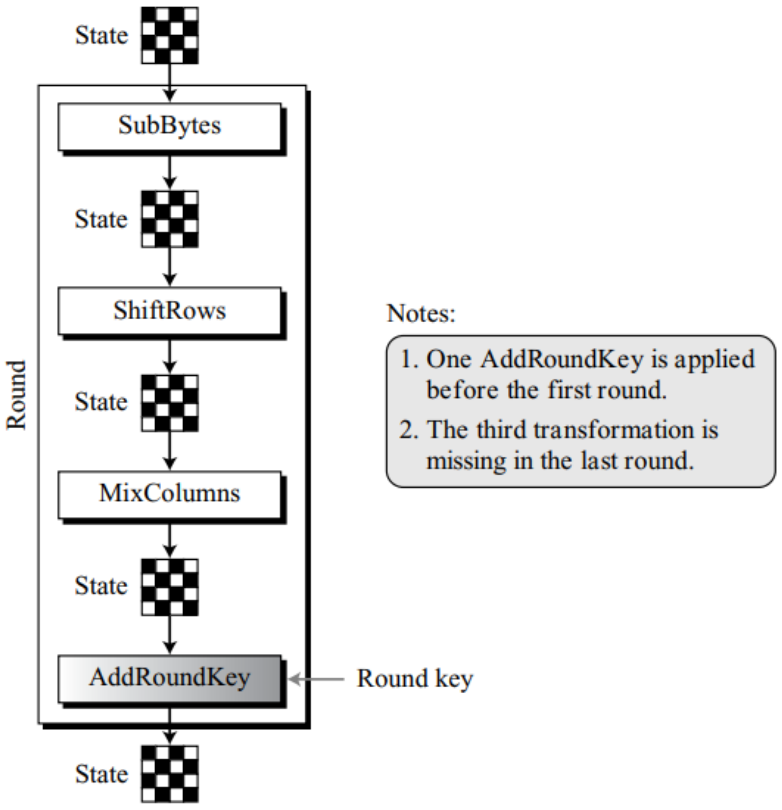


Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

The number of round keys generated by the key-expansion algorithm is always one more than the number of rounds. In other words, we have
Number of round keys = Nr + 1

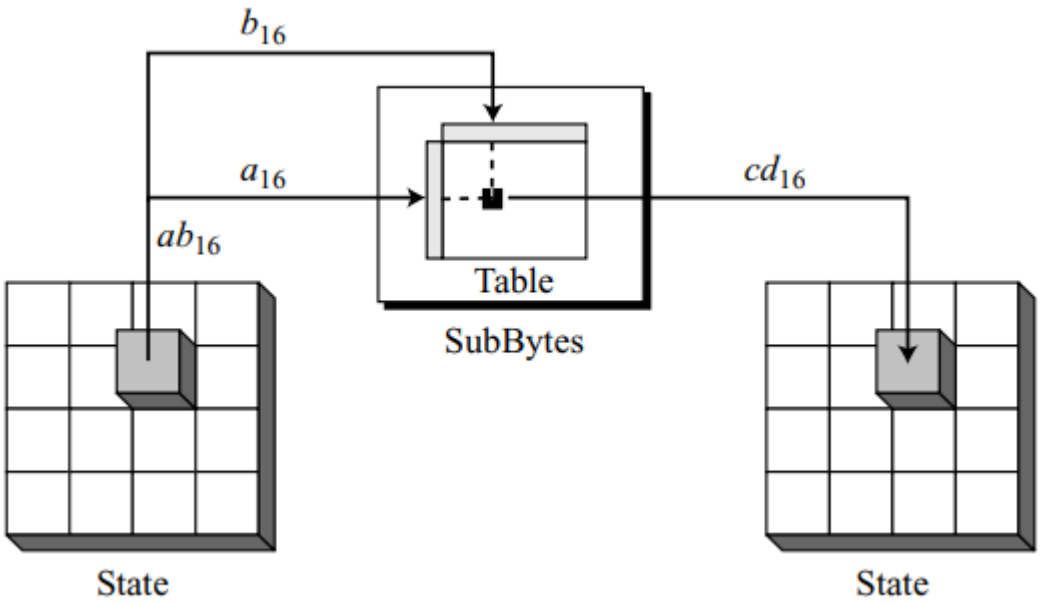
Figure 7.5 *Structure of each round at the encryption site*



SubBytes

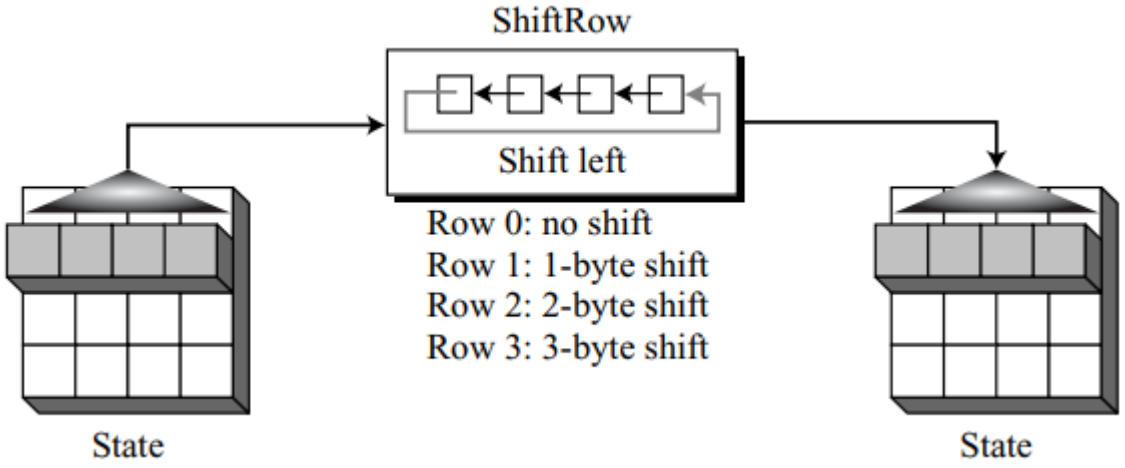
The first transformation, SubBytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits. The left digit defines the row and the right digit defines the column of the substitution table. The two hexadecimal digits at the junction of the row and the column are the new byte.

The SubBytes operation involves 16 independent byte-to-byte transformations.



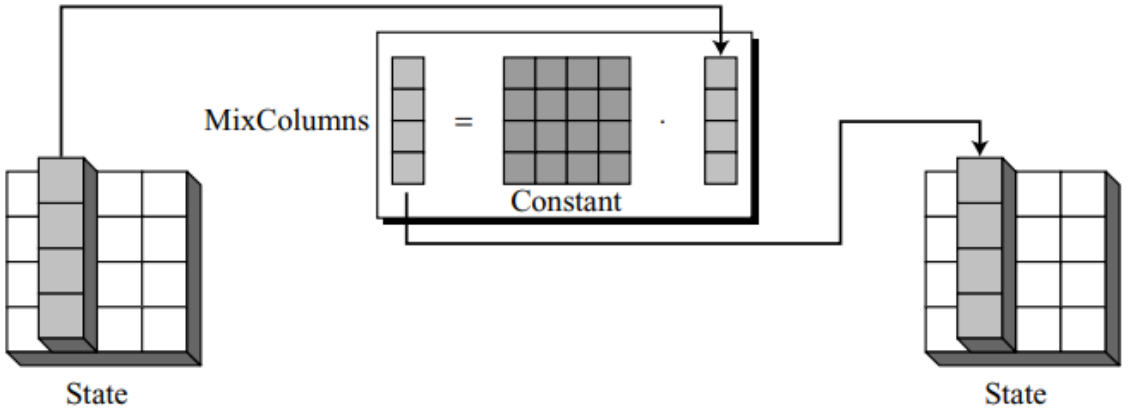
ShiftRows

In the encryption, the transformation is called ShiftRows and the shifting is to the left.The number of shifts depends on the row number (0, 1, 2, or 3) of the state matrix. This means the row 0 is not shifted at all and the last row is shifted three bytes.



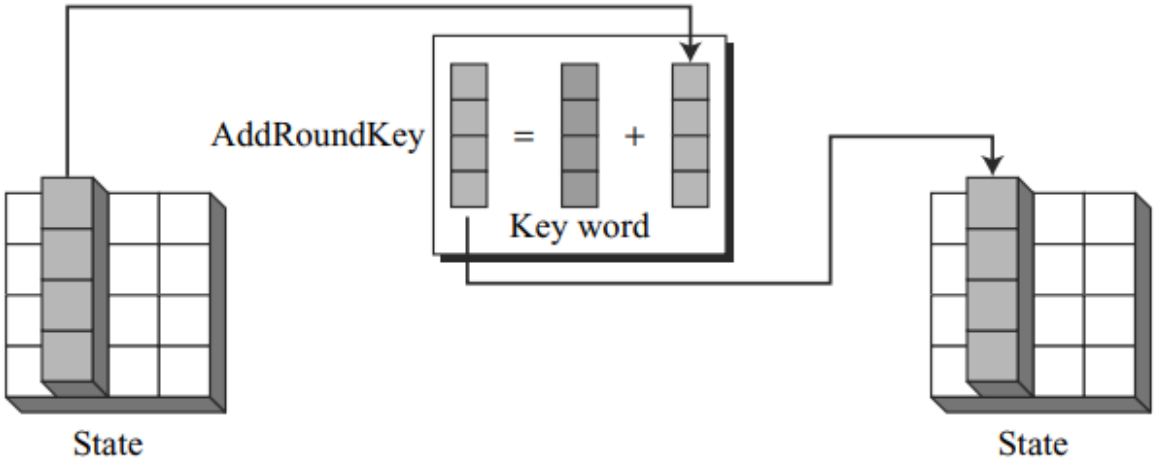
MixColumns

The MixColumns transformation operates at the column level; it transforms each column
of the state to a new column. The transformation is actually the matrix multiplication of a
state column by a constant square matrix



AddRoundKey

AddRoundKey also proceeds one column at a time. The AddRoundKey transformation can be thought as XORing of each column of the state, with the corresponding key word.



RC5 Algorithm

RC5 is a symmetric key block encryption algorithm designed by Ron Rivest in 1994. It is notable for being simple, fast (on account of using only primitive computer operations like XOR, shift, etc.) and consumes less memory.

RC5 is a block cipher and addresses two word blocks at a time. Depending on input plain text block size, number of rounds and key size, various instances of RC5 can be defined and each instance is denoted as RC5-w/r/b where w=word size in bits, r=number of rounds and b=key size in bytes. Allowed values are:

Parameter	Possible Value

block/word size (bits)	16, 32, 64
Number of Rounds	0 – 255
Key Size (bytes)	0 – 255

Advantages:

High level of security: RC5 is designed to provide a high level of security against attacks, including brute-force attacks and differential cryptanalysis. It uses a variable-length key and can operate on block sizes of up to 256 bits, making it difficult for attackers to break the encryption.

Fast encryption and decryption: RC5 is known for its fast encryption and decryption speeds. It uses simple mathematical operations such as modular arithmetic and bit shifting, which can be efficiently implemented on modern CPUs and hardware.

Flexible key length: RC5 allows for a variable-length key, which can range from 0 to 2040 bits. This flexibility allows users to choose a key length that suits their security needs and resources.

Disadvantages:

Vulnerable to side-channel attacks: RC5 is vulnerable to side-channel attacks, such as timing attacks and power analysis attacks. These attacks exploit information leaked through the implementation of the algorithm, rather than attacking the algorithm itself.

Limited adoption: RC5 is not widely adopted in practice compared to other encryption algorithms, such as AES. This means that there may be fewer resources and tools available to support RC5 in various applications and systems.

Patent issues: RC5 was subject to a patent held by RSA Security, which limited its adoption and use in commercial applications. Although the patent has since expired, it may have contributed to the limited adoption of RC5 compared to other encryption algorithms